WHAT IS CLAIMED IS:

1. A random number generator adapted to receive an input of a number of bits coming from a physical source, wherein the generator comprising, in combination:

at least one symbol-generating physical source;

an arithmetic encoder; and

smoothing means adapted to smooth the residual output biases.

2. The generator according to claim 1, wherein the smoothing means is constituted by a linear output function enabling the smoothing of the residual output biases.

3. The generator according to claim 1, wherein the arithmetic encoder comprises at least one table of statistics on the input symbols receiving a piece of information on contexts, several registers, one comparator and one logic unit.

4. The generator according to claim 1, wherein the smoothing means comprises a register, a serial input and a parallel output.

5. A method for the generation of random numbers comprising the following steps:

reception of several symbols from a physical source;

transmission of the symbols to an arithmetic encoder step; and

smoothing the encoded symbols using a linear function.

6. The method according to claim 5, further comprising encoding the symbols by a number derived from computations of nested intervals, an interval [ms, Ms] corresponding to a symbol s and having a size proportional to its frequency of occurrence.

7. The method according to claim 6, further comprising:

updating a table of statistics on the input symbols as a function of the contexts;

computing the new values of the boundaries of the interval [ms, Ms] by a rule of three; and

emptying the registers of the most significant bits that they have in common.

8. The method according to claim 6, wherein the encoding comprises the following steps:

1. initializing $m \rightarrow 0$ and $M \rightarrow 1$

2. updating, for each symbol s of the message to be compressed :

a. $\Delta \leftarrow M - m$;

b. $m \leftarrow m + \Delta \times m_s$;

c. $M \leftarrow m + \Delta \times M_s$

3. choosing the compressed message as being the last value of m.

9. The method according to claim 5 wherein the smoothing function makes use of a polynomial which is, at most, a 15th degree polynomial.

10. The method according to claim 2, wherein the arithmetic encoder comprises at least one table of statistics on the input symbols receiving a piece of information on contexts, several registers, one comparator and one logic unit.

11. The method according to claim 2, wherein the smoothing means comprises a register, a serial input and a parallel output.

12. The method according to claim 7, wherein the contexts are previous symbols.